

# Inhaltsverzeichnis

Vorwort .....	V
Vorwort zur 1. Auflage .....	VII
Abkürzungsverzeichnis .....	XIII
Literaturverzeichnis .....	XVII
<b>I. Einleitung .....</b>	<b>1</b>
<b>II. Rechtsquellen und Entwicklung der Datenschutzgesetzgebung .....</b>	<b>3</b>
1. Volkszählungsurteil des Bundesverfassungsgerichts („BVerfG“) .....	3
2. BDSG-Novellen seit Inkrafttreten des bisherigen BDSG aF .....	5
3. EU-Datenschutz-Grundverordnung .....	6
4. Persönlichkeitsschutz des Mitarbeiters .....	9
a) Recht am eigenen Bild .....	10
b) Recht am eigenen Wort .....	10
c) Recht am „geschriebenen“ Wort .....	11
<b>III. Kontrolle der betrieblichen Kommunikationsmittel .....</b>	<b>12</b>
1. Kontrolle von Internet und E-Mail .....	12
a) Anwendbarkeit des TKG und damit verbundene Beachtung des Fernmeldegeheimnisses im Arbeitsverhältnis .....	13
b) Kontrolle von Internet und E-Mail bei erlaubter Privatnutzung .....	17
aa) Entstehung eines Anspruchs des Mitarbeiters auf Privatnutzung .....	17
bb) Inhaltskontrolle von Mitarbeiter-E-Mails bei erlaubter Privatnutzung .....	19
cc) Auswertung der Verbindungsdaten von Internet- und E-Mail-Nutzung bei erlaubter Privatnutzung .....	22
dd) Strafrechtliche Risiken bei unzulässiger Kontrolle von Internet und E-Mail bei erlaubter Privatnutzung .....	25
ee) Praxistipps .....	27
c) Kontrolle von Internet und E-Mail bei ausschließlich dienstlicher Nutzung .....	28
aa) Inhaltskontrolle der Mitarbeiter-E-Mails bei ausschließlich dienstlicher Nutzung .....	29
bb) Auswertung der Verbindungsdaten von Internet- und E-Mail-Nutzung bei ausschließlich dienstlicher Nutzung .....	31
cc) Strafrechtliche Risiken bei unzulässiger Kontrolle von Internet und E-Mail bei ausschließlich dienstlicher Nutzung .....	33
dd) Praxistipps .....	34
d) Mitbestimmungsrechte des Betriebsrats .....	34
2. Telefonüberwachung .....	40
a) Telefonüberwachung bei erlaubter Privatnutzung .....	41
aa) Mithören und Aufzeichnen des Inhalts von Telefongesprächen bei erlaubter Privatnutzung .....	41
bb) Auswertung der Telefonverbindungsdaten bei erlaubter Privatnutzung .....	42
cc) Strafrechtliche Risiken bei unzulässiger Telefonüberwachung bei erlaubter Privatnutzung .....	44
dd) Praxistipps .....	44

b) Telefonüberwachung bei ausschließlich dienstlicher Nutzung .....	45
aa) Mithören und Aufzeichnen des Inhalts von Telefongesprächen bei ausschließlich dienstlicher Nutzung .....	45
bb) Auswertung der Verbindungsdaten der Telefonnutzung bei ausschließlich dienstlicher Nutzung .....	48
cc) Strafrechtliche Risiken bei unzulässiger Telefonüberwachung bei ausschließlich dienstlicher Nutzung .....	49
c) Mitbestimmungsrechte des Betriebsrats .....	50
<b>IV. Einsatz von Zeiterfassungs- und Zugangskontrollsystmen</b>	
<b>am Arbeitsplatz .....</b>	51
1. Einsatz von Zeiterfassungssystemen .....	52
2. Einsatz von Zugangskontrollsystmen .....	54
3. Mitbestimmungsrechte des Betriebsrats .....	56
<b>V. Videoüberwachung am Arbeitsplatz .....</b>	61
1. Eingesetzte Überwachungstechnik .....	63
2. Videoüberwachung von öffentlich zugänglichen Arbeitsplätzen .....	64
3. Einsatz offener Videoüberwachung .....	66
a) Abgrenzung von offener und verdeckter Videoüberwachung .....	66
b) Kenntlichmachung einer Videoüberwachung .....	67
c) Einsatz heimlicher Videoüberwachung .....	68
d) Die Rechtmäßigkeitsvoraussetzungen der Videoüberwachung im Einzelnen .....	72
aa) Videoüberwachung zur Durchführung des Beschäftigungsverhältnisses nach § 26 Abs. 1 S. 1 BDSG .....	73
bb) Videoüberwachung zur Aufklärung von Straftaten nach § 26 Abs. 1 S. 2 BDSG .....	74
e) Erforderlichkeit der Videoüberwachung .....	75
f) Verhältnismäßigkeit der Videoüberwachung .....	76
4. Mitbestimmungsrechte des Betriebsrats .....	79
<b>VI. Kontrollen ohne technische Hilfsmittel .....</b>	84
1. Tor- und Taschenkontrollen .....	84
2. Spindkontrollen .....	86
3. Einsatz von Privatdetektiven .....	88
4. Mitarbeiterinterviews .....	89
5. Mitbestimmungsrechte des Betriebsrats .....	93
<b>VII. Ortung der Mitarbeiter .....</b>	98
1. Darstellung einzelner Ortungssysteme .....	98
a) GPS .....	98
b) Handyortung .....	99
c) RFID .....	99
d) Digitaler Tachograf .....	100
2. Ortung bei dienstlicher Tätigkeit .....	100
a) Erhöhung der Verkehrssicherheit durch Kontrolle von Fahrzeiten .....	100
b) Ortung zur persönlichen Sicherheit des Arbeitnehmers .....	101
c) Präventive Abwehr von Straftaten durch Dritte gegen Mitarbeiter und Betriebsmittel des Arbeitgebers .....	102
d) Einsatz des Ortungssystems zur Einsatzkoordinierung der Arbeitnehmer .....	104
e) Einsatz des Ortungssystems zur Abwehr und Aufdeckung von Straftaten und Pflichtverstößen der eigenen Mitarbeiter .....	105

aa) Präventive Abwehr von Straftaten der Arbeitnehmer .....	106
bb) Aufklärung von bereits begangenen Straftaten der Mitarbeiter .....	106
cc) Aufklärung sonstiger Pflichtverstöße der Mitarbeiter .....	108
3. Ortung des Arbeitnehmers im Privatbereich .....	109
4. Mitbestimmungsrechte des Betriebsrats .....	109
<b>VIII. Gesundheits- und Eignungsuntersuchungen bei Mitarbeitern .....</b>	<b>114</b>
1. Eignungstests bei Bewerbern .....	114
a) Assessment-Center .....	115
b) Psychologische Tests .....	116
c) Graphologische Untersuchungen .....	117
2. Gesundheitsuntersuchungen im Bewerbungsverfahren .....	117
a) Ärztliche Untersuchungen vor der Einstellung .....	119
b) Genetische Untersuchungen .....	121
c) HIV- und AIDS-Tests .....	123
d) Drogen- und Alkoholtests .....	125
3. Eignungstests im bestehenden Arbeitsverhältnis .....	125
4. Gesundheitsuntersuchungen im bestehenden Arbeitsverhältnis .....	127
5. Mitbestimmungsrechte des Betriebsrats .....	128
<b>IX. Kontrolle der Social-Media-Aktivitäten der Mitarbeiter .....</b>	<b>130</b>
1. Abwehr von negativen Meinungsäußerungen und Beleidigungen im Web 2.0 .....	130
a) Äußerungen des Mitarbeiters nach Dienstschluss .....	131
b) Äußerungen des Mitarbeiters während der Arbeitszeit .....	133
c) Minimierung der Risiken durch Social Media Guidelines .....	133
2. Risiken des Verrats von Geschäfts- und Betriebsgeheimnissen im Web 2.0 .....	134
3. Unternehmensdarstellung im Web 2.0 aufgrund freiwilliger Initiative des Arbeitnehmers .....	136
a) Mögliche Risiken .....	136
b) Einflussmöglichkeiten des Arbeitgebers auf die Web 2.0-Nutzung .....	137
c) Minimierung der Risiken durch Social Media Guidelines .....	138
4. Unternehmensdarstellung im Web 2.0 aufgrund Verlangen des Arbeitgebers .....	139
a) Rechtmäßigkeit einer arbeitgeberseitigen Anordnung der dienstlichen Nutzung des Web 2.0 durch den Mitarbeiter .....	139
b) Einflussmöglichkeiten des Arbeitgebers bei der verpflichtenden Unternehmenspräsentation im Web 2.0 .....	140
c) Minimierung der Risiken durch Social Media Guidelines .....	140
5. Mitbestimmungsrechte des Betriebsrats .....	141
<b>X. Backgroundchecks von Bewerbern .....</b>	<b>148</b>
1. Abweichen von dem Grundsatz der Datendirekterhebung .....	148
2. Recherche über Internetsuchmaschinen .....	149
3. Recherche in sozialen Netzwerken .....	151
4. Beteiligungsrechte des Betriebsrats .....	154
<b>XI. Kontrolle von Terroristen .....</b>	<b>156</b>
1. Geltungsbereich und Regelungsinhalte der Verordnungen (EG) Nr. 2580/2001 und 881/2002 .....	156
2. Rechtmäßigkeit des Datenabgleichs .....	157

3. Verhältnismäßigkeit des Datenscreening .....	159
4. Mitbestimmungsrechte des Betriebsrats .....	160
5. Arbeitsrechtliche Folgen eines positiven Treffers auf der Terrorliste .....	161
<b>XII. Mitarbeiterkontrollen und Mitbestimmungsrechte des Betriebsrats ..</b>	<b>164</b>
1. Mitbestimmungsrecht des Betriebsrats bei technischer Überwachung nach § 87 Abs. 1 Nr. 6 BetrVG .....	164
2. Mitbestimmungsrecht des Betriebsrats bei Fragen der Ordnung des Betriebes und des Verhaltens der Arbeitnehmer nach § 87 Abs. 1 Nr. 1 BetrVG .....	166
3. Rechtfertigung von Mitarbeiterkontrollen durch Betriebsvereinbarung .....	167
<b>XIII. Überwachung des Betriebsrats ..</b>	<b>174</b>
1. Differenzierung zwischen Kontrollen der Betriebsratsmitglieder bei ihrer Amtsausübung und Überwachung von Betriebsratsmitgliedern bei Erbringung der Arbeitstätigkeit .....	174
2. Kontrolle der E-Mail- und Internetnutzung des Betriebsrats .....	176
3. Kontrolle der Telefonnutzung des Betriebsrats .....	178
4. Zeiterfassungskontrolle von Betriebsratsmitgliedern .....	180
5. Datenschutzrechtliche Kontrolle des Betriebsrats .....	182
<b>XIV. Wirksamkeit der Einwilligung eines Mitarbeiters in Kontrollen am Arbeitsplatz ..</b>	<b>185</b>
1. Form der Einwilligung .....	185
2. Freiwilligkeit der Einwilligungserklärung .....	186
3. Grundsatz der informierten Einwilligung/Konkretheit der Einwilligung .....	188
4. Widerrufbarkeit der Einwilligung .....	188
5. Kein Verstoß gegen zwingende Schutznormen oder höherrangiges Recht durch eine Einwilligung .....	189
6. Entwürfe für Einwilligungserklärungen .....	191
<b>XV. Folgen unzulässiger Mitarbeiterkontrollen ..</b>	<b>194</b>
1. Prozessuale Beweisverwertungsverbote bei unzulässigen Mitarbeiterkontrollen .....	194
a) Beweisverwertungsverbot wegen Verletzung des Persönlichkeitsrechts des Arbeitnehmers .....	195
b) Beweisverwertungsverbot wegen Verletzung der Mitbestimmungsrechte des Betriebsrats .....	196
2. Unterlassungs- und Beseitigungsansprüche des Arbeitnehmers .....	196
3. Zurückbehaltungsrecht des Arbeitnehmers .....	197
4. Bußgeldverfahren bei der Datenschutzaufsichtsbehörde sowie Schadensersatzansprüche des Arbeitnehmers .....	198
5. Rechte des Betriebsrats bei mitbestimmungswidrigen Mitarbeiterkontrollen .....	203
a) Unterlassungsanspruch des Betriebsrats nach § 23 Abs. 3 BetrVG ..	203
b) Allgemeiner Unterlassungsanspruch des Betriebsrats aus § 87 Abs. 1 BetrVG .....	204
<b>Sachverzeichnis ..</b>	<b>205</b>